Software & Information
Industry Association
1090 Vermont Ave NW Sixth Floor
Washington, DC 20005-4095

COMMENTS OF THE

SOFTWARE & INFORMATION INDUSTRY ASSOCIATION (SIIA)

To the request for comments on the

Proposed Recommendations of the President's President's Identity Theft Task Force (issued December 26, 2006)

On behalf of the members of the Software & Information Industry Association (SIIA), we appreciate this opportunity to submit our comments on the proposed recommendations that the President's Identity Theft Task Force is considering issuing "on ways to improve the effectiveness and efficiency of federal government efforts to reduce identity theft."

As the principal trade association of the software and digital information industry, the more than 750 members of SIIA develop and market software and electronic content for business, education, consumers and the Internet. SIIA's members are software companies, ebusinesses, and information service companies, as well as many electronic commerce companies. Our membership consists of some of the largest and oldest technology enterprises in the world, as well as many smaller and newer companies.

SIIA has been a leader in calling for coherent and meaningful national and regional frameworks for data security, including effective and meaningful security plans and breach notification. Our efforts have focused, in all cases, on the ultimate goal of promoting meaningful security practices, as well as combating the pernicious effects of identity theft, which costs both consumers and businesses billions of dollars each year.

Preliminary Observations

The recommendations published on December 26th appear to supplement a set of Interim Recommendations that were published by the Task Force on September 19, 2006. The Interim Recommendations, which have been in the public for several months now, focused on Prevention (specifically, improving

Tel: +1.202.289.7442
Fax: +1.202.289.7097
www.siia.net

government handling of sensitive personal data and improved authentication methods), Victim Assistance and Law Enforcement.

Our review of the document released on December 26th indicates that a number of new recommendations and new areas for proposals are put forward that were not included in the prior publication by the Task Force. A number of the proposals, highlighted below in our comments, have raised questions which we believe need to be carefully considered by the President's Task Force if its recommendations are to be useful and practical.

We note, in particular, that this latest set of recommendations has moved significantly from a focus on prevention that was exclusively government-centric to one where broad and sweeping recommendations are proposed that affect a vast array of private sector companies and entities. As our specific comments below indicate, several of the recommendations need substantial care in their articulation and should avoid reaching overbroad conclusions since little, if any, examination of the deeper issues has taken place with affected parties.

Specific Comments on Recommendations

Recommendation I.1 (Government Use of SSNs) and
Recommendation I.2 (Comprehensive Record on Private Sector Use of SSNs)

The Task Force is exploring ways to achieve reduced reliance on SSNs by all levels of government, and is considering exploring how SSNs are currently used in the private sector. In both cases, the Task Force is looking to reduce reliance on SSNs and make them less valuable in committing identity theft.

We strongly support the direction of the Task Force on this point. In our view, the Task Force should make it clear that SSNs should be used only as an identifier and never as an authenticator. The point of such a policy would be to reduce the fact that having someone's SSN no longer enables an ID thief to impersonate you; their knowing your SSN is simply another form of their knowing your name. It would be a very important step if the federal government says that SSN is an identifier only, and never an authenticator.

Recommendation I.3. (National Data Security Standards) The Task Force is apparently considering whether to recommend that "national data security requirements be imposed on all commercial entities that maintain sensitive consumer information," asking whether such a requirements would be helpful and if so, what would be the essential elements of the scheme?

There is a related proposal:

Recommendation I.4. (Breach Notice Requirements for Private Sector Entities Handling Sensitive Consumer Information) The Task Force is also considering whether to recommend that a "national breach notification requirement be adopted."

At the outset, it would be useful to examine the relationship between data security breaches and the incidence of identity theft. Despite wide spread publicity about data breaches, there is little documented evidence of the amount of "identity theft" – as currently defined by statute – that occurs as a result of data breaches. Part of this problem is that studies over time, have not used consistent definitions of breach, and many do not use legal definitions in defining their parameters.[1]

A close examination of several of the most publicized breaches illustrates the point. For example, in March 2005, a laptop with personal information on 98,369 graduate students or graduate-school applicants was stolen from the University of California at Berkeley. However, not a single case of stolen identity related to the incident was ever reported. "The laptop was recovered in September, and police believe that the thief was interested only in the computer, not in the information in its files."[2] In other cases, "it is unclear whether any breach had taken place, [although] there was the possibility that the information was accessed by unauthorized people."[3]

In one recent study, it was found that "data breaches were responsible for just 6 percent of all known cases of identity theft, compared to 30 percent from incidents like losing one's wallet. The study also showed that less than 1 percent of all individuals whose data was lost later became victims of ID theft."[4]

Thus, with the focus of the President's Task Force on identity theft, we urge the Task Force to carefully tread in its specific recommendations, which touch on a variety of areas related to security practices. In fact, a framework for promoting

---

[1] See, e.g., the methodology used by the ID Theft Resource Center. The Center compiles an on-going list of publicly reported breaches. The Center's website indicates that "Identity theft is a crime in which an imposter obtains key pieces of information such as Social Security and driver's license numbers and uses it for their own personal gain." However, the compilation provided by the Center includes many incidences that appear to not meet this particular definition.

[2] "Separating myth from reality in ID theft", CNET News.com, October 24, 2005, Found at: http://news.com.com/Separating+myth+from+reality+in+ID+theft/2100-1029_3-5907165.html.

[3] Michael, Turner, *Towards A Rational Personal Data Breach Notification Regime,* Information Policy Institute (June 2006), p. 8.

[4] "Survey: Data Breaches Yield Few ID Thefts", Computerworld, September 15, 2006. Found at: http://www.infoworld.com/article/06/09/15/HNidtheft_1.html.

security practices that address data security breaches is emerging, albeit one where the states have acted without a coherent approach.

One other point deserves elaboration, in light of the proposed recommendations focusing on the private sector. As the chart on the next page indicates, more than half of the breaches involve government agencies (including the military) and educational institutions (many of which are government institutions). General business accounted for 23%, while financial services and health care (which are directly affected by existing laws) accounted for 8% and 12%, respectively. We therefore urge that focus not be lost on the key role that government agencies play in promoting more effective security practices and steps that minimize the likelihood of data breaches:

Entity	**% of all in 2005**	**% of all in 2006**
Educational Institutions	48	27
Gov't\Military	12	30
Financial Serv	16	8
Health Care	11	12
General Business	13	23

Source: ID Theft Resource Center, 2006 Disclosures of U.S. Data Incidents, Updated 1/16/2007. Found at: http://www.idtheftcenter.org/breaches.pdf.

With regard to recommendation I.4, in the simplest terms, breach notification is one tool to respond to breaches when they occur; but, first and foremost, an effective framework should promote the development and implementation of on-going data security plans in a manner that promotes predictability and certainty for consumers, consumer protection authorities and businesses, and are appropriate to the circumstances of the data holder and type of information that is potentially at risk. The framework should provide for breach notification when there is, in fact, only a significant risk that identity theft has or is likely to occur. Without establishing a meaningful threshold and relevant requirements for notification, there is a very real likelihood of unintended, negative consequences for consumers, business entities and public authorities.

Lessons Learned from Existing Breach Notification Regimes

As the Task Force is probably aware, more than 35 state jurisdictions in the United States[5] have implemented data breach notification laws, and the U.S. Federal Trade Commission (FTC) is bringing actions under its existing authority[6] for failure to maintain or disclose security practices.[7] The following lessons, in our view, are emerging from the implementation of these regimes:

Establish a meaningful threshold for notification. To ensure that notification is part of a coherent approach to combating the pernicious effects of identity theft, a legal regime should require notification to consumers when the security of sensitive personal information has been breached in a manner that creates a ***significant risk*** of identity theft. This is the consistent recommendation of consumer protection authorities such as the FTC, for example. In testimony before the U.S. Congress, FTC Chairman Majoras stated the view of regulators that:

> " … companies … notify consumers when the security of this information has been breached in a manner that creates a significant risk of identity theft. Whatever language is chosen should ensure that consumers receive notices when they are at risk of identity theft, but not require notices to consumers when they are not at risk. … the goal of any notification requirement is to enable consumers to take steps to avoid the risk of identity theft. To be effective, any such requirement must provide businesses with adequate guidance as to when notices are required."[8]

---

[5] See, e.g., "State Security Breach Notification Laws (as of October 1, 2006)", found at: http://www.infosec.uga.edu/policymanagement/breachnotificationlaws.php.

[6] E.g., primarily Section 5 of the FTC Act for deceptive and unfair trade practices. See, also, Children's Online Privacy Protection Act (COPPA), Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act (FACTA).

[7] *See, e.g., In the Matter of CardSystems Solutions, Inc.,* FTC Docket No. C-4168 (Sept. 5, 2006); *In the Matter of DSW, Inc.,* FTC Docket No. C-4157 (Mar. 7, 2006); *United States v. ChoicePoint, Inc.,* No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006); *Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of BJ's Wholesale Club, Inc.,* FTC Docket No. C-4148 (Sept. 20, 2005). See, *also, Petco Animal Supplies, Inc.* (FTC Docket No. C-4133) (Mar. 4, 2005); *MTS Inc., d/b/a TowerRecords/Books/Video* (FTC Docket No. C-4110) (May 28, 2004); *Guess?, Inc.* (FTC Docket No. C-4091) (July 30, 2003); *Microsoft Corp.* (FTC Docket No. C-4069) (Dec. 20, 2002); *Eli Lilly & Co.* (FTC Docket No. C-4047) (May 8, 2002).

[8] Prepared Statement of the Federal Trade Commission on Data Breaches and Identity Theft, Presented by Chairman Majoras and the Other Members of the Commission Before the Committee on Commerce, Science, and Transportation of the United States Senate (June 16, 2005), p. 7. Found at: http://www.ftc.gov/os/2005/06/050616databreaches.pdf.

A meaningful threshold predicated on a "significant risk" standard is essential to avoid overnotification of consumers. As Chairman Majoras went on to outline in her testimony:

> "The challenge is to require notices *only* when there is a likelihood of harm to consumers. There may be security breaches that pose little or no risk of harm, such as a stolen laptop that is quickly recovered before the thief has time to boot it up. Requiring a notice in this type of situation might create unnecessary consumer concern and confusion. Moreover, if notices are required in cases where there is no significant risk to consumers, ***notices may be more common than would be useful***. As a result, ***consumers may become numb*** to them and fail to spot or act on those risks that truly are significant. In addition, ***notices can impose costs on consumers and on businesses,*** including businesses that were not responsible for the breach. For example, in response to a notice that the security of his or her information has been breached, a consumer may cancel credit cards, contact credit bureaus to place fraud alerts on his or her credit files, or obtain a new driver's license number. Each of these actions may be time-consuming for the consumer, and costly for the companies involved and ultimately for consumers generally."[9]

The establishment of a meaningful threshold is essential as there may be direct and harmful unintended consequences that may be associated with broad notification. For example, the experiences with notification regimes to date have demonstrated that consumers have been subjected to fraud scams and "phishing" attacks when bad actors hear through the media about notifications. The concern with consumers being preyed upon by bad actors in light of massive notification is a growing concern. In January 2006, the New York State Consumer Protection Board (CPB) advised that scam artists are now trying to cash in on the national paranoia over identity theft by luring victims with a phony warning that they may already be the victims of identity theft.[10] The FTC was compelled to caution U.S. veterans "to be extra careful of scams following the recent data breach at the Department of Veterans' Affairs (VA)," noting that "[i]n the past, fraudsters have used events like this to try to scam people into divulging their personal information by e-mail and over the phone."[11]

Such scams follow a simple, but serious pattern: Users may receive emails purporting to come from their credit card company or bank, referencing recent news reports of "breaches", asking them to enter their details and account

---

[9] Ibid, p. 10. (emphasis added)

[10] See "Phishing Fraudsters Prey on Identity Theft Fears," January 13, 2006, found at: http://www.consumeraffairs.com/news04/2006/01/cpb_phishing.html.

[11] "FTC Warns Veterans to Delete Unsolicited E-mails;*Scams via E-mail and Telephone Often Follow Data Breaches*," (June 2, 2006), found at: http://www.ftc.gov/opa/2006/06/fyi0632.htm.

numbers for the purposes of fraud protection or to reactivate their account. Often emails may even claim a fraud has been committed against the user's account and against the backdrop of the most recent data breach, many users will assume that news is legitimate.[12]

Define carefully the kind of personally identifiable information that is covered by notification requirements. Central to an effective framework is a meaningful definition of "sensitive personal information" that is relevant to combating the pernicious effects of identity theft. It is essential that a careful circumscribed set of "sensitive personal information" be the basis for determining whether any notification occurs.[13] It should not include elements that are widely used in commerce to facilitate transactions. It also makes no sense to require companies to impose additional security requirements on or notify consumers of security breaches on information that is already widely available and in the public domain.[14]

Avoid mandating specific technologies, while encouraging the adoption of good practices. SIIA would urge, as part of a coherent regional or national framework, technology-neutral incentives for businesses to take appropriate and effective steps to safeguard sensitive data. A number of security methods and practices are available to businesses and government, including encryption, truncation, access controls, anonymization and redaction. To single out one method to secure data in legislation, such as encryption, suggests, if not outright mandates a *de facto* exclusive means to avoid notification, creating a false sense of security. Singling out one methodology would not be in the overall best interests of the security marketplace, since it may reduce the development and use of diverse and innovative security tools.

Where 3rd parties manage data, and notification is required, avoid consumer confusion. In cases where a 3rd party manages "sensitive personal information" of consumers for entities that own or possess sensitive personal information, notification requirements should be constructed to avoid consumer confusion. The best way to achieve this end is to obligate the third party to notify the entity that owns or licenses the data – i.e., the entity that has the relationship

---

[12] See "Will MasterCard breach breed new wave of phishing?", 21 June 2005. Found at: http://software.silicon.com/security/0,39024655,39131331,00.htm.

[13] In general, sensitive personal information that, if breached, should be subject to notification, should include first and last name in combination with any of the following: (A) Government issued identification number used to facilitate social welfare benefits or the equivalent; or (B) Financial account number or credit card or debit card number of such individual, combined with any required security code, access code, or password that would permit access to such individual's account.

[14] It is noted that the vast majority of states that have enacted data security breach notification laws (31 of the 35 to date) have included an exception for public record information. These states include: AZ, CA, CO, CT, DE, FL, GA, HI, ID, IL, IN, KS, LA, ME, MI, MN, NE, NH, NC, ND, NJ, NY, NV, OH, PA, TN, TX, UT, VT, WA, and WI.

with the person whose sensitive personal information may have been breached. The entity that owns or licenses the sensitive personal information should, in turn, notify the end user or consumer. Otherwise, individuals are unlikely to recognize the source of the notice and thus unlikely to act in a manner to protect themselves, which is the object of notification regimes.

Promoting On-Going Security Plans

Based on our industry's experience, notification is one additional tool – but not the silver bullet – that can advance the goals of reducing misuse and abuse of information in the event of a breach of security. Instead, we urge that emphasis be placed on promoting on-going data security plans in a manner that promotes predictability and certainty for consumers, consumer protection authorities and businesses. We believe every company that collects sensitive information has an obligation to adopt and maintain sound data security practices. Implementing pre-breach security measures should be central to any federal framework on data breaches. Federal law should not simply require notification of consumers in case of a data breach. It should also require on-going security plans, as outlined below, to ensure the confidentiality and integrity of sensitive personal information in order to minimize the likelihood of a breach ever occurring in the first place.

SIIA offers the following principles to guide the development of policies that would form the basis for such an obligation, based on both international principles,[15] experts[16] and existing regimes.[17]

As a fundamental matter, the companies and entities that own or license sensitive personal information should develop a written information security plan that describes their program to protect such information. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the information it handles.[18] Stated another way,

---

[15] Organization for Economic Cooperation and Development (OECD), "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" (December 2005) ("OECD Guidelines"), found at: http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html.

[16] "Final Report of the Advisory Committee on Online Access and Security" (May 15, 2000)("Advisory Committee Final Report"), found at: http://www.ftc.gov/acoas/papers/finalreport.htm#III.

[17] Standards for Safeguarding Customer Information Rule ("Safeguards Rule"), 16 C.F.R. Part 314, issued pursuant to Title V of the Gramm-Leach-Bliley Act ("GLB Act"), 15 U.S.C. ' 6801 *et seq*..

[18] See, e.g., "Safeguards Rule." See, also, "OECD Guidelines", p. 12 ("Systems, networks and policies need to be properly designed, implemented and co-ordinated to optimise security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards

the promotion of on-going security plans should avoid micromanaging the details of the plans, since effective security plans will be based on risk and threat analysis, and implementation details that are unique to each entity's situation, taking into account a variety of factors that overt regulation cannot foresee or be flexible enough to adapt to in a rapid manner.

As a general matter, the experience to date suggests that each plan should include the following items, tailored to each entity's risk analysis and situation:

- designate one or more employees to coordinate its information security program;[19]
- identify and assess the risks to customer information in each relevant area of the company's operation (including, in particular) three areas that are particularly important to information security: employee management and training; information systems; detecting and managing system failures; and on-going evaluation of the effectiveness of the current safeguards for controlling these risks;[20]
- design and implement a safeguards program, and regularly monitor and test it;[21]

---

and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organisation's systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system."); "Advisory Committee Final Report", Sec. 3.4.4. ("…adopt security procedures (including managerial procedures) that are 'appropriate under the circumstances.' 'Appropriateness' would be defined through reliance on a case-by-case adjudication to provide context-specific determinations.")

[19] "Safeguards Rule", 16 C.F.R. 314.3(a).

[20] "Safeguards Rule", 16 C.F.R. 314.3(b). See, also, "OECD Guidelines" ("Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network security policies, practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements.")

[21] "Safeguards Rule", 16 C.F.R. 314.3(c). See, also, "OECD Guidelines" ("Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures. New and changing threats and vulnerabilities are continuously discovered. Participants should continually review, reassess and modify all aspects of security to deal with these evolving risks.")

- select service providers that can maintain appropriate safeguards, making sure that contracts with such service providers require them to maintain safeguards, and oversee their handling of customer information;[22] and
- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.[23]

To emphasize the experience of our industry to date: These requirements are designed to be flexible, be designed as appropriate to an entity's own circumstances and updated on an on-going basis. In addition, companies must consider and address any unique risks raised by their business operations — such as the risks raised when employees access customer data from their homes or other off-site locations, or when customer data is transmitted electronically outside the company network. These principles urge that rather than an overtly micromanaged legal regime, national or regional frameworks should obligate entities or companies to assess and address the risks to customer information in all areas of their operations and implement security plans accordingly.

Recommendation I.5. (Education of the Private Sector and Consumers on Safeguarding Data) We strongly urge the President's Task Force to highlight the need for education of both private sector entities, but also government entities as well as consumers. This should focus on how to avoid and protect their sensitive information – not merely, as the proposed recommendation suggests, on what they "should do if they suffer a data breach." We urge the recommendation to build on existing efforts, like those at the FTC (http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html) rather than starting from scratch.

Recommendation II (Preventing the Misuse of Consumer Data)

The Task Force noted, in its Interim Recommendation, that developing more reliable methods of authenticating the identities of individuals would make it harder for identity thieves to open new accounts or access existing accounts. In the latest proposals, the Task Force accordingly recommends that the Task Force hold workshops involving academics, industry and entrepreneurs, focused on developing and promoting improved means of authenticating the identities of individuals.

---

[22] "Safeguards Rule", 16 C.F.R. 314.3(d).

[23] "Safeguards Rule", 16 C.F.R. 314(e).

We support workshops that look at this issue. To be fully effective, the workshops must also explore only the means of authentication, but also the framework and business models for doing so. Based on our experience in the market, there will not be a one-size-fits-all approach to authenticating individuals. Rather, authentication will often depend on the specific context and circumstances in which is required and mechanisms implemented.

Recommendation IV.1 (Establish a National Identity Theft Law Enforcement Center) The proposed recommendations include a consideration of "whether to recommend the creation of a National Identity Theft Law Enforcement Center, to better coordinate the sharing of information among criminal and civil law enforcement and, where appropriate, the private sector." It goes without saying that coordination is essential. The relevant question is how best to do it. The Task Force summary recommendations have not examined the specific problem that is to be addressed. We note the recent FTC actions to centralize identity theft expertise in one unit of the agency. For the vast majority of our company members, the FTC is the primary federal agency we work with to combat the issues of identity theft. It is our understandings that, as appropriate, cases that rise to the level of criminal prosecution are forwarded to the U.S. Department of Justice. To the degree that a more visible point of contact with the private sector is necessary with the U.S. DOJ, we would encourage that step. In light of the distinction between civil and criminal responsibilities between agencies, we believe that further examination is warranted before moving to create a centralized Center as outlined in the proposed recommendations.

****

For further information on these comments, or if the Task Force has any questions, please contact:

Mark Bohannon
General Counsel & SVP Public Policy
Software & Information Industry Association (SIIA)
1090 Vermont Avenue, NW 6th Floor
Washington, DC 20005
Direct Line: 202-789-4471
Main Switchboard: 202-289-7442
Fax: 202-289-7097
Email: Mbohannon@siia.net

****